INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 512.6+519.725 https://doi.org/10.23947/1992-5980-2018-18-3-339-348

Differentiation of polynomials in several variables over Galois fields of fuzzy cardinality and applications to Reed-Muller codes*

V. M. Deundyak[1,2], N. S. Mogilevskaya[2]**

[1] Research Institute "Spetsvuzavtomatika", Rostov-on-Don, Russian Federation.
[2] Southern Federal University, Rostov-on-Don, Russian Federation

Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида-Маллера***

В. М. Деундяк[1,2], Н. С. Могилевская[2]**

[1] НИИ «Спецвузавтоматика», г. Ростов-на-Дону, Российская Федерация.
[2] Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация.

Introduction. Polynomials in several variables over Galois fields provide the basis for the Reed-Muller coding theory, and are also used in a number of cryptographic problems. The properties of such polynomials specified over the derived Galois fields of fuzzy cardinality are studied. For the results obtained, two real-world applications are proposed: partitioning scheme and Reed-Muller code decoder.

Materials and Methods. Using linear algebra, theory of Galois fields, and general theory of polynomials in several variables, we have obtained results related to the differentiation and integration of polynomials in several variables over Galois fields of fuzzy cardinality. An analog of the differentiation operator is constructed and studied for vectors.

Research Results. On the basis of the obtained results on the differentiation and integration of polynomials, a new decoder for Reed-Muller codes of the second order is given, and a scheme for organizing the partitioned transfer of confidential data is proposed. This is a communication system in which the source data on the sender is divided into several parts and, independently of one another, transmitted through different communication channels, and then, on the receiver, the initial data is restored of the parts retrieved. The proposed scheme feature is that it enables to protect data, both from the nonlegitimate access, and from unintentional errors; herewith, one and the same mathematical apparatus is used in both cases. The developed decoder for the second-order Reed-Muller codes prescribed over the derived odd Galois field may have a constraint to the recoverable error level; however, its use is advisable for a number of the communication channels.

Введение. Полиномы нескольких переменных над полями Галуа лежат в основе теории кодов Рида-Маллера, а также используются в ряде криптографических задач. В работе изучаются свойства таких полиномов, заданных над произвольными полями Галуа нечетной мощности. Для полученных результатов предложены два практических приложения: схема разделения данных и декодер кодов Рида-Маллера.

Материалы и методы. С использованием линейной алгебры, теории полей Галуа и общей теории полиномов нескольких переменных получены результаты, связанные с дифференцированием и интегрированием полиномов нескольких переменных над полями Галуа нечетной мощности. Для векторов построен и изучен аналог оператора дифференцирования.

Результаты исследования. На основе полученных результатов о дифференцировании и интегрировании полиномов предложен новый декодер для кодов Рида-Маллера второго порядка и предложена схема организации разделенной передачи конфиденциальных данных, т.е. такой системы связи, в которой исходные данные на стороне отправителя разделяются на несколько частей и, независимо друг от друга, передаются по различным каналам связи, а на стороне получателя из принятых частей восстанавливаются исходные данные. Особенностью предлагаемой схемы является то, что она позволяет защищать данные, как от нелегитимного доступа, так и от непреднамеренных ошибок, при этом в обоих случаях используется один и тот же математический аппарат. Разработанный декодер для кодов Рида-Маллера второго порядка, заданных над произвольным нечетным полем Галуа, может иметь некоторое ограничение по числу исправляемых ошибок, однако, его использование целесообразно для ряда каналов связи.

* The research is done within the frame of independent R&D.
** E-mail: vl.deundyak@gmail.com, nadezhda.mogilevskaia@yandex.ru
*** Работа выполнена в рамках инициативной НИР.

Discussion and Conclusions. The proposed practical applications of the results obtained are useful for the organization of reliable communication systems. In future, it is planned to study the restoration process of the original polynomial by its derivatives, in case of their partial distortion, and the development of appropriate applications.

Обсуждение и заключения. Предложенные практические приложения полученных результатов представляются полезными для организации надежных систем связи. В дальнейшем планируется исследование процесса восстановления исходного полинома по его производным, в случае их частичного искажения, и разработка соответствующих приложений.

Keywords: polynomials in several variables, Galois fields, polynomial derivatives, differentiation of polynomials, Reed-Muller codes, decoding, partitioned data transmission.

Ключевые слова: полиномы нескольких переменных, поля Галуа, производные полиномов, дифференцирование полиномов, коды Рида-Маллера, декодирование, разделенная передача данных.,

For citation: V. M. Deundyak, N. S. Mogilevskaya. Differentiation of polynomials in several variables over Galois fields of fuzzy cardinality and applications to Reed-Muller codes. Vestnik of DSTU, 2018, vol. 18, no.3, pp. 339–348. https://doi.org/10.23947/1992-5980-2018-18-3-339-348

Образец для цитирования: Деундяк, В. М. Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида-Маллера / В. М. Деундяк, Н. С. Могилевская // Вестник Дон. гос. техн. ун-та. — 2018. — Т. 18, № 3. — С. 339–348. https://doi.org/10.23947/1992-5980-2018-18-3-339-348

Introduction. Polynomials of several variables over Galois fields and their derivatives are used in several information security domains. Some issues on the integration and differentiation of polynomials of several variables are considered in a number of papers. Thus, in [1], polynomials defined over simple Galois fields are studied, in [2-4], results for Boolean functions are obtained, and in [5-6], results for polynomials given over ternary Galois fields are described.

In this paper, we consider polynomials of several variables specified over the derived Galois fields of fuzzy cardinality. For such polynomials, the results related to the calculation of the directional derivatives, as well as to the restoration of the polynomial from the set of its derivatives calculated in the basic directions are obtained. For the results, two possible practical applications are proposed: a partitioning scheme and a decoder for Reed-Muller codes (PM codes).

The partitioning scheme can be used to organize the partitioned transmission of confidential data, i.e. such a communication system in which the initial data on the sender is divided into several parts and, independently of one another, transmitted through different communication channels, and then, on the receiver, the original data is restored from the collected parts. The proposed scheme feature is that it enables to protect data, both from the nonlegitimate access, and from unintentional errors. At this, in both cases, one and the same mathematical apparatus associated with PM codes and polynomial differentiation is used. Partitioned transmission can be used both to improve the communication speed, and to ensure data security by complicating the task of interception from several communication lines. Some issues on data partition are considered in [7-11].

For PM-codes of the second order, deterministic decoders are known only for certain values of the Galois field cardinality q. Such as, quite a lot of decoders are known for the case of $q = 2$, for example [12-13], for the case of $q = 3$ and the use of a semicontinuous communication channel, a decoder [5] is constructed. In [14], a second-order Reed-Muller decoder for the codes preset over Galois fields of cardinality 2, 4, and 8 is proposed. The second-order PM code decoder defined above the derived fuzzy Galois field proposed in this paper is based on reduction to first-order Reed-Muller codes. Their codewords can be decoded by any suitable decoder. In the case of PM codes specified over the fields with cardinality of more than three, the proposed decoder has some limitation on the recoverable error rate. It should be mentioned that the use of the proposed decoding scheme in case of field cardinality of more than three, may be advisable at a low noise pollution level of the communication channels used despite the limitation.

Differentiation of polynomials in several variables

Suppose $q = p^s$, where p is an odd prime, $s \in \mathrm{N}$, F_q is a Galois field of q cardinality. Let us consider a polynomial ring in m variables $\mathrm{F}_q[x_1,...,x_m]$ over F_q field. Let us denote the polynomial linear space of $\mathrm{F}_q[x_1,...,x_m]$ degree not more than r as $\mathrm{F}_q^{(r)}[x_1,...,x_m]$. Suppose F_q^m is m-linear space over F_q.

The result of the differentiation operator action is the polynomial derivative $f \in \mathrm{F}_q^{(r)}[x_1,...,x_m]$ along $\bar{b} \in \mathrm{F}_q^m$:

$$(D_{\bar{b}} f)(\bar{x}) = f_{\bar{b}}(\bar{x}) - f(\bar{x}), \quad \bar{x} \in \mathrm{F}_q^m, \tag{1}$$

where $f_{\bar{b}}(\bar{x}) = f(\bar{x} + \bar{b})$. It is easy to see that $D_{\bar{b}} f \in \mathrm{F}_q^{(r-1)}[x_1,...,x_m]$, and the operator

$$D_{\bar{b}} f : \mathrm{F}_q^{(r)}[x_1,...,x_m] \to \mathrm{F}_q^{(r-1)}[x_1,...,x_m] \tag{2}$$

is a linear one. Let us denote the vector coordinate sum $\bar{\alpha} \in \mathrm{F}_p^m$, where p is prime, as a sum of natural numbers, by $\rho(\bar{\alpha})$. The polynomials $f \in \mathrm{F}_q^{(2)}[x_1,...,x_m]$ may be written in a canonical form

$$f(\bar{x}) = \sum_{\bar{\alpha} \in \mathrm{F}_q^m} f_{\bar{\alpha}} \bar{x}^{\bar{\alpha}} = a_{\bar{0}} \bar{x}^{\bar{0}} + \sum_{\rho(\bar{\alpha})=1} a_{\bar{\alpha}} \bar{x}^{\bar{\alpha}} + \sum_{\rho(\bar{\alpha})=2} a_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}, \tag{3}$$

where, when writing the monomial $\bar{x}^{\bar{\alpha}} = x_1^{\alpha_1} ... x_m^{\alpha_m}$, the indices α_i will be identified with the elements of the field F_p, and the summands in each sum will be arranged in an lexicographic order of magnitude. If the last sum in (3) is zero, we obtain a polynomial in $\mathrm{F}_q^{(1)}[x_1,...,x_m]$.

Lemma 1. Suppose $q = p^s$, p is an odd prime, $f(\bar{x}) \in \mathrm{F}_q^{(2)}[x_1,...,x_m]$ is a polynomial in a canonical form (3), $\bar{b} = (b_1,...,b_m) \in \mathrm{F}_q^m$. Then

$$f(\bar{x}) = f_{00...00} + \bar{x}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x} A \bar{x}^T, \tag{4}$$

$$(D_{\bar{b}} f)(\bar{x}) = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + 2\bar{x} A \bar{b}^T + \bar{b} A \bar{b}^T = 2\bar{x} A \bar{b}^T + f(\bar{b}) - f_{00...00}, \tag{5}$$

where

$$A = \begin{pmatrix} f_{200..00} & f_{110..00}/2 & f_{101..00}/2 & \cdots & f_{100..10}/2 & f_{100..01}/2 \\ f_{110..00}/2 & f_{020..00} & f_{011..00}/2 & \cdots & f_{010..10}/2 & f_{010..01}/2 \\ f_{101..00}/2 & f_{011..00}/2 & f_{002..00} & \cdots & f_{001..10}/2 & f_{001..01}/2 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \cdots \\ f_{100..10}/2 & f_{010..10}/2 & f_{001..10}/2 & \cdots & f_{000..20} & f_{000..11}/2 \\ f_{100..01}/2 & f_{010..01}/2 & f_{001..01}/2 & \cdots & f_{000..11}/2 & f_{000..02} \end{pmatrix},$$

Proof. In the case of a prime Galois field, the proof is contained in [1]. Using (1), (4) and matrix symmetry, we obtain:

$$f_{\bar{b}}(\bar{x}) = f(\bar{x}+\bar{b}) = f_{00...00} + (\bar{x}+\bar{b})\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + (\bar{x}+\bar{b}) A (\bar{x}+\bar{b})^T,$$

$$(D_{\bar{b}} f)(\bar{x}) = f_{\bar{b}}(\bar{x}) - f(\bar{x}) = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x} A \bar{b}^T + \bar{b} A \bar{x}^T + \bar{b} A \bar{b}^T,$$

$$(D_{\bar{b}} f)(\bar{x}) = \bar{b}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + 2\bar{x} A \bar{b}^T + \bar{b} A \bar{b}^T = 2\bar{x} A \bar{b}^T + f(\bar{b}) - f_{00...00}. \bullet$$

Let us prove the theorem that determines the restoring method up to a polynomial constant term in $\mathrm{F}_q^{(2)}[x_1, x_2, ..., x_m]$ by the set of its derivatives calculated in the basic directions.

Theorem 1. Suppose $\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i)\}_{i=1,...,m}$ is some basis of space F_q^m, where q is odd. Let us consider the polynomial $f \in \mathrm{F}_q^{(2)}[x_1, x_2, ..., x_m]$ of (4):

$$f(\bar{x}) = f_{00...00} + \bar{x}\left(f_{10...00}, f_{01...00}, ..., f_{00...01}\right)^T + \bar{x} A \bar{x}^T.$$

If

$$\left\{\left(D_{\bar{b}_i} f\right)(\bar{x}) = \alpha_1^i x_1 + \alpha_2^i x_2 + ... + \alpha_m^i x_m + \alpha_0^i\right\}_{i=1,...,m}, \tag{6}$$

Then,

$$A = \frac{1}{2} \begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \cdots & \alpha_1^m \\ \alpha_2^1 & \alpha_2^2 & \cdots & \alpha_2^m \\ \vdots & \cdots & \ddots & \vdots \\ \alpha_m^1 & \alpha_m^2 & \cdots & \alpha_m^m \end{pmatrix} \begin{pmatrix} b_1^1 & b_1^2 & \cdots & b_1^m \\ b_2^1 & b_2^2 & \cdots & b_2^m \\ \vdots & \cdots & \ddots & \vdots \\ b_m^1 & b_m^2 & \cdots & b_m^m \end{pmatrix}^{-1}, \tag{7}$$

$$\begin{pmatrix} f_{10...00} \\ f_{01...00} \\ \vdots \\ f_{00...01} \end{pmatrix} = \begin{pmatrix} \alpha_0^1 - \bar{b}_1 A \bar{b}_1^T \\ \alpha_0^2 - \bar{b}_2 A \bar{b}_2^T \\ \vdots \\ \alpha_0^m - \bar{b}_m A \bar{b}_m^T \end{pmatrix} \begin{pmatrix} b_1^1 & b_2^1 & \cdots & b_m^1 \\ b_1^2 & b_2^2 & \cdots & b_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1^m & b_2^m & \cdots & b_m^m \end{pmatrix}^{-1}. \tag{8}$$

Proof. From (5), (6), we obtain:

$$\forall\ i=1,\ ...,\ m:\ 2A\bar{b}_i^T=(\alpha_1^i,\alpha_2^i,...,\alpha_m^i)^T,\ f(\bar{b}_i)-f_{00..00}=\alpha_0^i. \quad (9)$$

Then,

$$2A\begin{pmatrix} b_1^1 & b_1^2 & \cdots & b_1^m \\ b_2^1 & b_2^2 & \cdots & b_2^m \\ \vdots & \vdots & \ddots & \vdots \\ b_m^1 & b_m^2 & \cdots & b_m^m \end{pmatrix}=\begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \ldots & \alpha_1^m \\ \alpha_2^1 & \alpha_2^2 & \ldots & \alpha_2^m \\ \vdots & \ldots & \ddots & \vdots \\ \alpha_m^1 & \alpha_m^2 & \cdots & \alpha_m^m \end{pmatrix}.$$

Hence, the formula (7) comes out right.

It follows from (4) that for any $\bar{b}\in \mathrm{F}_q^m$:

$$f(\bar{b})-f_{00..00}=\bar{b}\left(f_{10...00},f_{01...00},...,f_{00...01}\right)^T+\bar{b}A\bar{b}^T.$$

For $\bar{b}$, we take the vectors $\bar{b}_i\in\beta$ and use the equation $f(\bar{b}_i)-f_{00..00}=\alpha_0^i$ from (9). Then,

$$\forall\ i=1,\ ...,\ m:\ \alpha_0^i-\bar{b}_i A\bar{b}_i^T=\bar{b}_i\left(f_{10...00},f_{01...00},...,f_{00...01}\right)^T.$$

Consequently,

$$\begin{pmatrix} \alpha_0^1-\bar{b}_1A\bar{b}_1^T \\ \alpha_0^2-\bar{b}_2A\bar{b}_2^T \\ \vdots \\ \alpha_0^m-\bar{b}_mA\bar{b}_m^T \end{pmatrix}=\begin{pmatrix} b_1^1 & b_2^1 & \cdots & b_m^1 \\ b_1^2 & b_2^2 & \cdots & b_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1^m & b_2^m & \cdots & b_m^m \end{pmatrix}\begin{pmatrix} f_{10...00} \\ f_{01...00} \\ \vdots \\ f_{00...01} \end{pmatrix}$$

And the formula (8) is proved. •

Reed-Muller q-ary codes $RM_q(r,m)$. Let us consider RM-codes over the finite field F_q where $q=p^s$, p is an odd prime, $s\in\mathrm{N}$ [15–16]. The elements $\mathrm{F}_q^{(r)}[x_1,...,x_m]$ are information polynomials of the code $RM_q(r,m)$; we suppose that $m\ge r>0$, $m\ge 2$. Vector $\bar{f}$ made up from the information polynomial coefficients is called an information vector.

In the vector space F_q^m, let us fix some ordering

$$\{\bar{\alpha}_1,\ ...,\ \bar{\alpha}_n\}\ (\bar{\alpha}_j=(\alpha_{j1},\alpha_{j2},...,\alpha_{jm}))\ ,\ n=q^m. \quad (10)$$

The arbitrary information polynomial $f(\bar{x})\in\mathrm{F}_q^{(r)}[x_1,...,x_m]$ is coded by its evaluation at the ordered space F_q^m points:

$$C(f)=(f(\bar{\alpha}_1),...,f(\bar{\alpha}_n)), \quad (11)$$

and so, the coder-operator is defined

$$C:\ \mathrm{F}_q^{(r)}[x_1,...,x_m]\to\mathrm{F}_q^n.$$

Reed-Muller codes are defined by the natural parameters r and m (r<m)

$$RM_q(r,m)=\{(f(\bar{\alpha}_1),...,f(\bar{\alpha}_n))\,|\,f(\bar{x})\in\mathrm{F}_q[x_1,...,x_m],\deg(f)\le r\}\subset\mathrm{F}_q^n,$$

The parameter *r* is called a code order. They form a family of linear [n, k, d] q-codes whose length and dimension are determined from the formulas

$$n=q^m,\ \ k=\sum_{i=0}^{r}\sum_{j=0}^{\lfloor i/q\rfloor}(-1)^j C_m^j C_{i-qj+m-1}^{m-1},$$

where $\lfloor\ \rfloor$ is rounding up to the smaller whole number, and the minimum code distance d of the code $RM_q(r,m)$ is convenient to calculate using the dual code $RM_q(r^\perp,m)$ parameters where $r^\perp=m(q-1)-r-1$. Suppose ρ is residue of division $r^\perp+1$ by $q-1$: $r^\perp+1=\sigma(q-1)+\rho$ where $\rho<q-1$, then the parameter d of the code $RM_q(r,m)$ is given by the expression

$$d=(\rho+1)q^\sigma. \quad (12)$$

Note that the arbitrary [n, k, d] $_q$-code enables to correct $t=\lfloor(d-1)/2\rfloor$ errors in one codeword [17].

Next, let us consider PM-codes of orders 1 and 2 given over Galois fields of fuzzy cardinality, write the corresponding information polynomials in the form (3), and use ordering (10) for numbering the information vector coordinates.

Lemma 2. Let $r \in \{1;2\}$, $q \geq 3$, then the minimum code distance of the code $RM_q(r,m)$ is calculated by the formula:

$$d_r = (q-r)q^{m-1}, \tag{13}$$

and values of the recoverable $t_r = \lfloor (d-1)/2 \rfloor$ - by the codes $RM_q(r,m)$, $r \in \{1;2\}$, are related as follows:

$$t_1/2 \leq t_2. \tag{14}$$

Proof. Let us make use of the fact that $r < q$ and calculate σ and ρ - subquotient and the remainder of the division $r^{\perp}+1$ by $q-1$ respectively:

$$\sigma = (m(q-1)-r)\operatorname{div}(q-1) = m-1;$$

$$\rho = (m(q-1)-r)\bmod(q-1) = q-1-r.$$

Then, from the formula (12) we obtain (13). From the equalities $d_1 = (q-1)q^{m-1}$, $d_2 = (q-2)q^{m-1}$, we get that the desired inequality (14) is as follows

$$\frac{1}{2}\cdot\left\lfloor \frac{(q-1)q^{m-1}-1}{2} \right\rfloor \leq \left\lfloor \frac{(q-2)q^{m-1}-1}{2} \right\rfloor.$$

Note that d_2 is odd, and d_1 is even, hence

$$\left\lfloor \frac{(q-2)q^{m-1}-1}{2} \right\rfloor = \frac{(q-2)q^{m-1}-1}{2},$$

$$\left\lfloor \frac{(q-1)q^{m-1}-1}{2} \right\rfloor = \frac{(q-1)q^{m-1}-2}{2},$$

Consequently, the inequality (14) takes the form

$$\frac{1}{2}\left(\frac{(q-1)q^{m-1}-2}{2}\right) \leq \frac{(q-2)q^{m-1}-1}{2},$$

It is easily seen that it is equal to the inequality $q \geq 3$. •

Consequence. If q>3, then there is a strict and when q=3, then there is an equality in (14).

Table 1 lists parameters of some PM-codes. The top three lines contain the parameters q, m, n of the code in question $RM_q(r,m)$. The following three lines contain the values: k_1 is code dimension, d_1 is minimum code distance, and t_1 is the number of recoverable errors for the codes $RM_q(1,m)$. And the following three lines show similar values of k_2, d_2, t_2 for the codes $RM_q(2,m)$.

Table 1

Parameter values of some RM-codes

q		3				5				7			
m		2	3	5	7	2	3	5	7	2	3	4	5
n		9	27	243	2187	25	125	3125	78125	49	343	2401	16807
r=1	k_1	3	4	6	8	3	4	6	8	3	4	5	6
	d_1	6	18	162	1458	20	100	2500	62500	42	294	2058	14406
	t_1	2	8	80	728	9	49	1249	31249	20	146	1028	7202
r=2	k_2	6	10	21	36	6	10	21	36	6	10	15	21
	d_2	3	9	81	729	15	75	1875	46875	35	245	1725	12005
	t_2	1	4	40	364	7	37	937	23437	17	122	857	6002

Now, we introduce the analog of the differentiation operator $D_{\bar{b}}$ operating in the space of polynomials (see (2)), for the space F_q^n where $n = q^m$. The vector coordinates from F_q^n will be numbered by vectors from the ordered set F_q^m (see (10)). Let us consider the shift operator $\tau_{\bar{b}} : \mathrm{F}_q^n \to \mathrm{F}_q^n$ following the formula

$$\tau_{\bar{b}}(\bar{a}) = (a_{\bar{\alpha}_1 + \bar{b}}, ..., a_{\bar{\alpha}_n + \bar{b}}),$$

where $\bar{a} = (a_{\bar{\alpha}_1}, ..., a_{\bar{\alpha}_n}) \in \mathrm{F}_q^n$, $\bar{b} = (b_1, ..., b_m) \in \mathrm{F}_q^m$. Note that the shift operator $\tau_{\bar{b}}$ is mixing bijection. The linear operator $\Delta_{\bar{b}} : \mathrm{F}_q^n \to \mathrm{F}_q^n$, that is the analog to $D_{\bar{b}}$, is defined by the formula:

$$\Delta_{\bar{b}}(\bar{a}) = \tau_{\bar{b}}(\bar{a}) - \bar{a},\ \bar{a} = (a_{\bar{\alpha}_1}, ..., a_{\bar{\alpha}_n}) \in \mathrm{F}_q^n. \quad (15)$$

We call $\Delta_{\bar{b}}(\bar{a})$ a vector derivative of vector $\bar{a}$ along $\bar{b}$.

Lemma 3. Let us consider the polynomial $f \in \mathrm{F}_q^{(2)}[x_1, x_2, ..., x_m]$, vector $\bar{b} = (b_1, ..., b_m) \in \mathrm{F}_q^m$, operators $\Delta_{\bar{b}}$, $D_{\bar{b}}$ and C. Then,

$$\tau_{\bar{b}}(C(f)) = C(f_{\bar{b}}),\ C(D_{\bar{b}} f) = \Delta_{\bar{b}}(C(f)). \quad (16)$$

The proof is carried out by the direct calculations, and for $q = 3$ is available in [6].

Note that from (2) and (16), it follows that if $C(w) \in RM_q(2, m)$, then $\Delta_{\bar{b}}(C(w)) \in RM_q(1, m)$.

Below, we consider examples of practical applications of the theoretical results obtained.

Data partitioning scheme. For partitioning and restoring data in the proposed scheme, we use $[n, k_1, d_1]_q$-code, $RM_q(1, m)$ and $[n, k_2, d_2]_q$-code $RM_q(2, m)$, specified over the derived Galois field F_q of fuzzy cardinality. Values q and m are parameters of this scheme.

Data partitioning algorithm.

Input: information vector $\bar{w} \in \mathrm{F}_q^{k_2}$ of the code $RM_q(2, m)$ and an ordered set of basic vectors

$$\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathrm{F}_q^m\}_{i=\overline{1,...,m}}, \quad (17)$$

That is a private key of the scheme under consideration.

Output: vectors $\bar{S}_i \in \mathrm{F}_q^{n+1}$, $i = \overline{1, m}$.

Step 1. Let us assign the information polynomial $w = w(\bar{x})$ to the input vector $\bar{w}$ and encode it using (11) into the vector $C(w) \in \mathrm{F}_q^n$ of the code $RM_q(2, m)$.

Step 2. Let us form m of the vector derivatives (see (15)):

$$\Delta_{\bar{b}_i}(C(w)) = C(D_{\bar{b}_i}(w)) \in \mathrm{F}_q^n,\ i = \overline{1, m},\ \bar{b}_i \in \beta.$$

Note that $C(D_{\bar{b}_i}(w)) \in RM_q(1, m)$.

Step 3. We concatenate each vector $C(D_{\bar{b}_i}(w)) \in \mathrm{F}_q^n$, $i = \overline{1, m}$ with the coefficient $f_{00..00} := w(\bar{0})$ of the code vector $C(w)$:

$$\bar{S}_i = C(D_{\bar{b}_i}(w)) \,||\, f_{00..00} \in \mathrm{F}_q^{n+1}.$$

Then, vectors $\bar{S}_i \in \mathrm{F}_q^{n+1}$, $i = \overline{1, m}$ are transmitted along m different communication lines. Obviously, during the transmission, vectors $\bar{S}_i$, $i = \overline{1, m}$ can be distorted. Thus, from the communication channel, vectors $\bar{S}_i'$ will be obtained:

$$\bar{S}_i' = (C(D_{\bar{b}_i}(w)))' \,||\, f'_{00..00} \in \mathrm{F}_p^{n+1},\ i = \overline{1, m}.$$

where $(C(D_{\bar{b}_i}(w)))'$ is supposedly distorted vector $C(D_{\bar{b}_i}(w))$, scalar $f'_{00..00}$ is supposedly distorted value $f_{00..00}$. Let us denote scalar $f'_{00..00}$ corresponding to $\bar{S}_i'$ by $f'_{00..00\,i}$.

Data recovery algorithm.

Input: vectors $\bar{S}_i'$, $i = \overline{1, m}$ and private key β (see (17)).

Output: vector $\bar{w}' \in \mathrm{F}_q^{k_2}$.

Step 1. We isolate two components: $(C(D_{\bar{b}_i}(w)))' \in \mathrm{F}_q^n$ and $f'_{00..00\,i}$, $i = \overline{1, m}$ from each vector $\bar{S}_i'$, $i = \overline{1, m}$.

Step 2. We direct the vectors $(C(D_{\bar{b}_i}(w)))'$ to the decoders of the code $RM_q(1, m)$. Note that you can use arbitrary decoders, for example, [16], [18]. At the output of the decoders considered, polynomials $D'_{\bar{b}_i}(w) \subset \mathrm{F}_q^{(1)}[x_1, x_2, ..., x_m]$, $i = 1, ..., m$ are generated.

Step 3. We develop vector $(f'_{00..00,1}, f'_{00..00,2}, ..., f'_{00..00,m})$ from the coefficients $f'_{00..00,i}$ and feed it to the decoder input of the code $RM_q(0, m)$ which actually coincides with the code of m-tuple repetition. The result of this decoder performance is the scalar $f''_{00..00}$.

Step 4. We substitute the values of the coefficients of the polynomials $D_{\bar{b}_i}^{'}(w) \subset \mathrm{F}_q^{(1)}\left[x_1, x_2, ..., x_m\right]$, $i = \overline{1,m}$ and the key β (see (17)) into the formulas (7) and (8), and derive the polynomial $f(\bar{x})$ from the results obtained. Then we calculate the desired polynomial $w'(\bar{x}) = f(\bar{x}) + f_{00..00}^{''}$.

Step 5. The message recipient is given the information vector $\bar{w}' \in \mathrm{F}_q^k$ corresponding to the polynomial $w'(\bar{x})$.

Note 1. The correctness of the data recovery algorithm depends on the number of errors that damage the vectors $\bar{S}_i \in \mathrm{F}_q^{n+1}$ during their transmission along the communication lines, as well as on the correcting capacity of the first-order PM-codes used. It is plain that if the decoders used reconstruct the vectors $C(D_{\bar{b}_i}(w))$ and the value $f_{00..00}$ correctly, then the initial data restoration using the results of Theorem 1 will be correct, hence the vector $w'(\bar{x})$ obtained at the output of the data recovery algorithm will coincide with the original information vector $\bar{w} \in \mathrm{F}_q^{k_2}$. Note that operation of the decoder for recovery $C(D_{\bar{b}_i}(w))$ is correct, if

$$\forall i = \overline{1,m}: \; d_h(C(D_{\bar{b}_i}(w)), (C(D_{\bar{b}_i}(w)))') \le \lfloor (d_1 - 1)/2 \rfloor,$$

where $d_h(\bar{x}, \bar{y})$ is Hamming distance between the vectors $\bar{x}, \bar{y}$. The scalar $f_{00..00}$ is restored correctly if the vector $(f_{00..00,1}^{'}, f_{00..00,2}^{'}, ..., f_{00..00,m}^{'})$ formed in step 3 of the algorithm contains fewer than m/2 coordinates differing from the value $f_{00..00} = w(\bar{0})$. If, in $\bar{S}_i \in \mathrm{F}_q^{n+1}, i = \overline{1,m}$, more errors occurred than can be restored by the decoders used, then the recovery $\bar{w} \in \mathrm{F}_q^{k_2}$ is not guaranteed.

Note 2. The proposed partition and recovery algorithms employ Reed-Muller codes of both the first and second orders, but the decoders are used only for the first-order codes.

Note 3. The transmission confidentiality is provided not only by the need for knowledge of the key, but also by using several communication lines, because in this case, data interception is more challenging for an intruder than illegal data capture from a single communication line.

Decoder of Reed-Muller codes of the second order. First, let us consider the idea of the decoding algorithm organization, and then we describe the algorithm step-by-step. Let us fix some basis $\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathrm{F}_\mathrm{q}^\mathrm{m}\}_{i=1,...,m}$ in the space $\mathrm{F}_\mathrm{q}^\mathrm{m}$ where $q = p^s$, p is an odd prime. Suppose that the decoder input receives $\bar{Y} = C(w) + \bar{e} \; (\in \mathrm{F}_q^n)$ where w is the information polynomial, $C(w)$ is the code vector of the $[n, k_2, d_2]_q$-code, $RM_q(2,m)$, $\bar{e} \in F_q^n$ is the error vector for which

$$wt_h(\bar{e}) \le t_2, \tag{18}$$

where $wt_h(.)$ is Hamming weight, $t_2 = \lfloor (d_2 - 1)/2 \rfloor$. Employing vector $\bar{Y}$, we construct m vector derivatives calculated in the basic directions using the operator $\Delta_{\bar{b}}$:

$$\Delta_{\bar{b}_i}(\bar{Y}) = \Delta_{\bar{b}_i}(C(w) + \bar{e}) = \Delta_{\bar{b}_i}(C(w)) + \Delta_{\bar{b}_i}(\bar{e}), \; i = 1, ..., m$$

each of which is the vector $\Delta_{\bar{b}_i}(C(w)) \in RM_q(1,m)$ distorted by the error vector $\Delta_{\bar{b}_i}(\bar{e}) \in \mathrm{F}_q^n$, and can be unerringly decoded by an arbitrary decoder of the $[n, k_1, d_1]_q$-code $RM_q(1,m)$ operating up to half the code distance (see, e.g., [16], [18]), if the error level is less than $t_1 = \lfloor (d_1 - 1)/2 \rfloor$, i.e. when

$$wt_h(\Delta_{\bar{b}_i}(\bar{e})) \le t_1. \tag{19}$$

If the vectors are decoded correctly, then the desired information polynomial of the code can be reconstructed using Theorem 1 up to one coordinate which can be then found, for example, by maximum likelihood decoding. Thus, for proper decoding $\bar{Y}$, according to the proposed scheme, the fulfillment of the condition (19) is required.

Algorithm for decoding the code $RM_q(2,m)$.

Input: parameters of $[n, k_2, d_2]_q$-code $RM_q(2,m)$, $\bar{Y} = (Y_{\alpha_1}, Y_{\alpha_2}, ...Y_{\alpha_n}) \in \mathrm{F}_q^n$.

Output: decoded information vector $\bar{w}$.

Step 1. Let us fix some basis $\beta = \{\bar{b}_i = (b_1^i, b_2^i, ..., b_m^i) \in \mathrm{F}_\mathrm{q}^\mathrm{m}\}_{i=1,...,m}$ of the space $\mathrm{F}_\mathrm{q}^\mathrm{m}$ and calculate the derived vectors along all the directions $\bar{b}_i \in \beta$:

$$\Delta_{\bar{b}_i}(\bar{Y}) = \tau_{\bar{b}_i}(\bar{Y}) - \bar{Y}.$$

Step 2. Let us decode $\Delta_{\bar{b}_i}(\bar{Y})$, $i = 1, ..., m$, using the arbitrary decoder of $RM_q(1,m)$-codes that operates up to half the code distance, and as a result, we obtain vectors $\bar{p}_{\bar{b}_i}$ and their polynomial representations

$$p_{\bar{b}_i}(\bar{x}) = \alpha_1^i x_1 + \alpha_2^i x_2 + ... + \alpha_m^i x_m + \alpha_0^i \subset \mathrm{F}_p^{(1)}\left[x_1, x_2, ..., x_m\right], \; i = 1, ..., m.$$

Step 3. Using the polynomials $p_{\bar{b}_i}(\bar{x})$, $i = 1,...,m$, we find the polynomial $f(\bar{x})$ with the intercept zeroth-order term from the formulas (7) and (8).

Step 4. For all $z \in \mathrm{F}_q$, we calculate

$$\Psi(z) = \sum_{i=1}^{n} \left| C(f(\bar{x}) + z)_{\alpha_i} - Y_{\alpha_i} \right|,$$

where $C(f(\bar{x}) + z)_{\alpha_i}$ is α_i - th coordinate of the vector $C(f(\bar{x}) + z)$ (see (11)). Let us denote z_0 the value z on which the function $\Psi(z)$ attained its minimum.

Step 5. The decoding result is vector $\bar{w}$ that one-to-one corresponds to the information polynomial $w(\bar{x}) = f(\bar{x}) + z_0$.

Theorem 2. So that the derived algorithm of decoding the code $RM_q(2,m)$ can rectify all errors, it is sufficient to meet the conditions (18) and

$$wt_h(\bar{e}) \le t_1 / 2, \tag{20}$$

where $t_1 = \lfloor (d_1 - 1)/2 \rfloor$, d_1 is minimum distance of the code $RM_q(1,m)$.

Proof. At step 2, the decoder input receives vectors

$$\Delta_{\bar{b}_i}(\bar{Y}) = \tau_{\bar{b}_i}(\bar{Y}) - \bar{Y} = \tau_{\bar{b}_i}(C(\bar{w})) + \tau_{\bar{b}_i}(\bar{e}) - C(\bar{w}) - \bar{e} = \Delta_{\bar{b}_i}(C(w)) + \Delta_{\bar{b}_i}(e).$$

Recall that $\Delta_{\bar{b}_i}(C(w)) \in RM_q(1,m)$, and the decoders of the code $RM_q(1,m)$ operating up to half the code distance rectify up to t_1 errors in the codeword. From the condition (20), it follows that

$$wt_h(\Delta_{\bar{b}_i}(\bar{e})) \le wt_h(\tau_{\bar{b}_i}(\bar{e})) + wt_h(\bar{e}) = 2wt_h(\bar{e}) \le t_1$$

So, vectors $\bar{p}_{\bar{b}_i}$ which are developed at Step 2 coincide with $\Delta_{\bar{b}_i}(C(w))$. Hence it follows that at Step 3, owing to Theorem 1, the polynomial $f(\bar{x}) = w(\bar{x}) - w(\bar{0})$ is formed.

From the condition (18), it follows that the value z_0 calculated at Step 4 is equal to the constant term $w(\bar{0})$ of the desired information polynomial $w(\bar{x})$. Thus, the desired information vector $\bar{w}$ is obtained.

Note that for the correct decoding according to the proposed scheme, it is required to meet the condition (20), from which (19) follows, although the condition (18) is more natural. Let us consider the relationship between these conditions.

Lemma 4. For the codes $RM_q(2,m)$, in the case of $q = 3$, the condition (18) and (20) are equivalent, and in the case of $q > 3$, when the condition (18) is satisfied, the fulfillment of the condition (20) is not guaranteed.

Proof. From the consequence of Lemma 2, we obtain that at $q = 3$, the equality $t_1/2 = t_2$ is true; i.e. the right-hand sides of the inequalities (18) and (20) coincide; hence, the fulfillment of one of them implies the fulfillment of the other. At $q > 3$ from the consequence of Lemma 2, we obtain that $t_1/2 < t_2$, viz from the fulfillment of (18), the fulfillment of (20) does not follow.

Note 1. In [5-6], the decoder of the $RM_3(2,m)$-code is described, where, as in the proposed algorithm, derivative vectors are constructed for the noisy codeword. They are decoded by the maximum likelihood algorithm, and then the desired information word is restored from the values obtained. However, the derived vectors are constructed in all 3^m possible directions, not only in basic ones, in the decoder from [5-6]. And another mechanism is used to obtain the desired information vector.

Note 2. For codes $RM_q(2,m)$, $q = 3$, the proposed decoder operates up to half the code distance. For codes $RM_q(2,m)$, $q > 3$, the proposed decoder does not guarantee the correction of all errors, the number of which is less than t_2, but the decoder will operate well if the weaker condition (20) is satisfied. Note that the use of the proposed decoding scheme in case of the fields with cardinality of more than three may be appropriate, despite the determined limitation, for the following reasons. First, the theory of the decoders of the second-order PM-codes is ill-defined. But, if there is a first-order decoder, then the proposed decoder which is a suspension over it can fill in this gap. Secondly, when using the communication channels, the error probability in which is such that (20) is satisfied, the transition from the first-order PM-codes to the second-order codes reduces redundancy (see Table 1).

Conclusion. Theoretical results associated with restoring polynomials of several variables over Galois fields of fuzzy cardinality by their derivatives are obtained. As practical applications to the results obtained, a data partition scheme and a second-order PM-code decoder are proposed. In future, it is instructive to study the process of a polynomial recovery from distorted derivatives, and to develop appropriate modifications of the real-world applications proposed in this paper.

References

1. Deundyak, V.M., Knutova, A.V. Integriruemost' sistem polinomov neskol'kikh peremennykh pervoy i vtoroy stepeni nad prostymi polyami Galua. [Integrability of systems of the first and second degree polynomials of several variables over simple Galois fields.] Izvestiya vuzov. Severo-Kavkazskiy region. Natural Sciences. 2016, no. 2, pp. 41–46 (in Russian).

2. Ambrosimov, A.S. Svoystva bent-funktsiy q-znachnoy logiki nad konechnymi polyami. [Properties of bent-functions of q-valued logic over finite fields.] Discrete Mathematics, 1994, no. 3(6), pp. 50–60 (in Russian).

3. Logachev, O.A., Salnikov, A.A., Yashchenko, V.V. Bulevy funktsii v teorii kodirovaniya i kriptologii. [Boolean functions in coding theory and cryptology.] Moscow: MTsNMO, 2004, 470 p. (in Russian).

4. Mazurenko, A.V., Mogilevskaya, N.S. Sposob vosstanovleniya bulevoy funktsii neskol'kikh peremennykh po ee proizvodnoy. [Method of restoring multivariable Boolean function from its derivative.] Vestnik of DSTU, 2017, no. 1 (88), pp. 122–131 (in Russian).

5. Deundyak, V.M., Mogilevskaya, N.S. Model' troichnogo kanala peredachi dannykh s ispol'zovaniem dekodera myagkikh resheniy kodov Rida-Mallera vtorogo poryadka. [The model of the ternary communication channel with using the decoder of soft decision for Reed-Muller codes of the second order.] University News. North-Caucasian region. Technical Sciences Series, 2015, no. 1 (182), pp. 3–10 (in Russian).

6. Deundyak, V.M., Mogilevskaya, N.S. Ob usloviyakh korrektnosti dekodera myagkikh resheniy troichnykh kodov Rida-Mallera vtorogo poryadka. [On correctness conditions of s soft-decisions decoder for ternary Reed-Muller codes of the second order.] Vladikavkaz Mathematical Journal, 2016, vol. 18, iss. 4, pp. 23–33 (in Russian).

7. Mogilevskaya, N.S., Kulbikayan, R.V., Zhuravlev, L.A. Porogovoe razdelenie faylov na osnove bitovykh masok: ideya i vozmozhnoe primenenie. [Threshold file sharing based on bit masks: concept and possible use.] Vestnik of DSTU, 2011, vol.11, no. 10, pp. 1749–1755 (in Russian).

8. Tormasov, A.G., Khasin, M.A., Pakhomov, Y.I. Obespechenie otkazoustoychivosti v raspredelennykh sredakh. [Fault tolerance in distributed environments.] Programming, 2001, vol. 27, no. 5, pp. 26 (in Russian).

9. Mishchenko, V.A., Vilanskiy, Y.V. Ushcherbnye teksty i mnogokanal'naya kriptografiya. [Distorted texts and multichannel cryptography.] Minsk: Entsiklopediks, 2007, 292 p. (in Russian).

10. Deundyak, V.M., Popova, S.B. Model' organizatsii zashchishchennogo dokumentooborota na baze raspredelennoy peredachi dannykh s autentifikatsiey. [Secure document management model based on distributed data transmission with authentication.] Vestnik of DSTU, 2015, vol. 15, no. 4, pp. 101–106 (in Russian).

11. Mogilevskaya, N.S. O primenenii porogovogo razdeleniya dannykh dlya organizatsii razdelennoy peredachi na primere metoda bitovykh masok. [On application of threshold data partitioning for organization of split transmission using bitmask method as an example.] Engineering Journal of Don, 2017, no. 2. Available at: http://www.ivdon.ru/uploads/article/pdf/IVD_48_ Mogilevskaya.pdf_492254b6f1.pdf (accessed :12.08.2017) (in Russian).

12. Sidelnikov, V.M., Pershakov, A.S. Dekodirovanie kodov Rida-Mallera pri bol'shom chisle oshibok. [Decoding of Reed-Muller codes with a large number of errors.] Problems of Information Transmission, 1992, vol. 28, no. 3, pp. 80–94 (in Russian).

13. Karyakin, Yu.D. Bystroe korrelyatsionnoe dekodirovanie kodov Rida—Mallera. [Fast correlation decoding of Reed-Muller codes.] Problems of Information Transmission, 1987, vol. 23, no. 2, pp. 40–49 (in Russian).

14. Paterson, K.G., Jones, A.E. Efficient decoding algorithms for generalized Reed-Muller codes. IEEE Transactions on Communications, 2000, vol. 48, iss. 8, pp. 1272 – 1285.

15. Pellikaan, R., Wu, X.-W. List decoding of q-ary Reed-Muller Codes. IEEE Trans. On Information Theory, 2004, vol. 50, iss. 3, pp. 679-682.

16. Santhi, N. On Algebraic Decoding of q-ary Reed-Muller and Product Reed-Solomon Codes. ISIT 2007 Conference, June 24 -29, Nice, France, 2007.

17. Deundyak, V.M., Maevskiy, A.E., Mogilevskaya, N.S. Методы помехоустойчивой защиты данных [Methods of noisefree data protection.] Rostov-on-Don: SFU, 2014, 309 p. (in Russian).

18. Ashikhmin, A.E., Litsyn, S.N. Fast Decoding of Non-Binary First Order Reed-Muller Codes. Applicable Algebra in Engineering, Communication and Computing, 1996, vol. 7, iss. 4, pp. 299–308.

Received 08.11.2017
Submitted 09.12.2017
Scheduled in the issue 21.06.2018

Authors:

Deundyak, Vladimir M.,
associate professor of the Algebra and Discrete Mathematics Department, Vorovich Institute for Mathematics, Mechanics, and Computer Science, Southern Federal University, Senior Research Scholar, Southern Regional Certification Centre, Research Institute "Spetsvuzavtomatika" (51, Gazetny per., Rostov-on-Don, 344002, RF), Cand(Phys-Math), associate professor,
ORCID: http://orcid.org/0000-0001-8258-2419
vl.deundyak@gmail.com

Mogilevskaya, Nadezhda S.,
associate professor of Vorovich Institute for Mathematics, Mechanics, and Computer Science, Southern Federal University (8-a, ul. Milchakova, Rostov-on-Don, 344090, RF), Cand(Eng), associate professor,
ORCID: http://orcid.org/0000-0003-1357-5869
nadezhda.mogilevskaia@yandex.ru